19-1204

IN THE

United States Court of Appeals

FOR THE FOURTH CIRCUIT

FRANK HEINDEL; PHIL P. LEVENTIS,

Plaintiffs-Appellants,

—v.—

MARCI ANDINO, Executive Director of the South Carolina State Election Commission, in her official capacity; JOHN WELLS, Chair of the South Carolina State Election Commission, in his official capacity; CLIFFORD J. ELDER, AMANDA LOVEDAY, SCOTT MOSELY, Members of the South Carolina State Election Commission, in their official capacity,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA AT COLUMBIA

BRIEF FOR PLAINTIFFS-APPELLANTS

LAURENCE M. SCHWARTZTOL
PROTECT DEMOCRACY PROJECT, INC.
125 Walnut Street, Suite 202
Watertown, Massachusetts 02472
(202) 945-2092

JESSICA A. MARSDEN
PROTECT DEMOCRACY PROJECT, INC.
510 Meadowmont Village Circle,
No. 328
Chapel Hill, North Carolina 27517
(202) 672-4812

DAVID S. FRANKEL
HARRY P. MORGENTHAU
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
(212) 715-9100

JAMILA G. BENKATO
PROTECT DEMOCRACY PROJECT, INC.
2020 Pennsylvania Avenue, NW,
No. 163
Washington, DC 20006
(202) 579-4582

Attorneys for Plaintiffs-Appellants

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 19-1204 Caption: Frank Heindel v. Marci Andino

Pursuant to FRAP 26.1 and Local Rule 26.1,

Frank Heindel
(name of party/amicus)

who is Appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

You created this PDF from an application that is not licensed to print to novaPDF printer (http://www.novapdf.com)

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/ David Stanley Frankel Date: 3/12/2019

Counsel for: Appellants

CERTIFICATE OF SERVICE

****

I certify that on March 12, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

OFFICE OF THE ATTORNEY GENERAL OF
SOUTH CAROLINA
P.O. Box 11549
Columbia, SC 29211-1549

/s/ David Stanley Frankel (signature) 03/12/2019 (date)

You created this PDF from an application that is not licensed to print to novaPDF printer (http://www.novapdf.com)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER INTERESTS

Disclosures must be filed on behalf of all parties to a civil, agency, bankruptcy or mandamus case, except that a disclosure statement is **not** required from the United States, from an indigent party, or from a state or local government in a pro se case. In mandamus cases arising from a civil or bankruptcy action, all parties to the action in the district court are considered parties to the mandamus case.

Corporate defendants in a criminal or post-conviction case and corporate amici curiae are required to file disclosure statements.

If counsel is not a registered ECF filer and does not intend to file documents other than the required disclosure statement, counsel may file the disclosure statement in paper rather than electronic form. Counsel has a continuing duty to update this information.

No. 19-1204 Caption: Frank Heindel v. Marci Andino

Pursuant to FRAP 26.1 and Local Rule 26.1,

Phil P. Leventis
(name of party/amicus)

who is Appellant, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

You created this PDF from an application that is not licensed to print to novaPDF printer (http://www.novapdf.com)

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))? ☐ YES ☑ NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☑ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☑ NO
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/ David Stanley Frankel Date: 3/12/2019

Counsel for: Appellants

CERTIFICATE OF SERVICE

****

I certify that on March 12, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

OFFICE OF THE ATTORNEY GENERAL OF
SOUTH CAROLINA
P.O. Box 11549
Columbia, SC 29211-1549

/s/ David Stanley Frankel (signature) 03/12/2019 (date)

You created this PDF from an application that is not licensed to print to novaPDF printer (http://www.novapdf.com)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

Plaintiffs Frank Heindel and Phil Leventis are South Carolina voters who simply want their votes to be counted. When they go to the polls each Election Day, they cast their ballots on antiquated voting machines that produce no paper record of their votes. For more than 10 years, Defendants, the executive director and commissioners of the South Carolina State Election Commission, have known that this voting system is susceptible to hacking. The system—a "dinosaur," in the words of one local election official—also regularly malfunctions, including in ways that cause votes not to be counted. Now, as national-security experts report that the risk of attacks against American election systems has reached a crisis level and as the machines themselves continue to deteriorate, the risk that Plaintiffs' votes will be lost is substantial. Yet Defendants continue to rely on these machines to record and count Plaintiffs' votes, including in upcoming elections.

This impermissibly infringes Plaintiffs' right to vote, the most "precious" right in any democracy. *Wesberry v. Sanders*, 376 U.S. 1, 17 (1964). Courts have long understood that when plaintiffs allege a substantial risk of future injury, like the one faced by Plaintiffs here, they have standing to seek prospective relief from the courts. This is particularly true for plaintiffs challenging unconstitutional election procedures, where it is typically impossible to say in advance which voters will be disenfranchised and where remedying the violation after an election is

almost always impossible. As long as plaintiffs have plausibly alleged facts to support their claim that their votes have a substantial risk of being put in jeopardy, courts have permitted them to proceed past the pleading stage.

Plaintiffs here have more than satisfied that burden. The Complaint alleges, in detail, the many well-known flaws in the design of South Carolina's voting machines, which expose those machines to a high risk of attack by hackers. Indeed, leading security researchers studying the voting system in place in South Carolina have demonstrated its susceptibility to attacks that can "propagate virally" through the system's architecture to affect elections on a large scale. Through simulated attacks, those same researchers demonstrated directly that the system can be hacked. In addition to the risk of hacking, the voting system maintained by Defendants has suffered numerous mechanical failures, including failures that lead to lost votes and other inaccuracies. The Complaint also details the consensus among U.S. national-security and intelligence officials that our election systems are squarely in the crosshairs of foreign adversaries, and that paperless voting machines like those used in South Carolina face the greatest risk.

The District Court erred by holding Plaintiffs to an inappropriately high standard. Rather than decide whether Plaintiffs plausibly alleged a substantial risk that their voting rights would be impaired, the District Court devoted the bulk of its opinion to analyzing whether that harm is "certainly impending." But establishing

standing based on the risk of future injury does not require demonstrating a certainly impending injury in all cases. The Supreme Court has repeatedly stated that plaintiffs may have a cognizable injury based on a substantial risk of future harm. Applying the Supreme Court's precedent, numerous lower courts have emphasized that plaintiffs asserting voting rights claims need not establish that harm is certainly impending when they are able to establish a substantial risk that their right to vote will be denied. The District Court compounded its error by demanding a level of proof beyond what is required at the motion-to-dismiss stage, ignoring this Court's admonition not to "blur[] the line between the distinct burden for establishing standing at the motion-to-dismiss and summary-judgment stages of litigation." *Wikimedia Found. v. NSA*, 857 F.3d 193, 212 (4th Cir. 2017). Plaintiffs' claims are supported by detailed factual allegations that more than plausibly support their claim that Defendants' policies burden their right to vote. Under well-established law, Plaintiffs' allegations are sufficient to support their standing.

JURISDICTIONAL STATEMENT

The District Court had jurisdiction over this action under 28 U.S.C. § 1331 and 42 U.S.C. § 1983. The court granted Defendants' motion to dismiss and entered final judgment on February 8, 2019. This Court has appellate jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF ISSUES

1. Whether, at the motion-to-dismiss stage, voting-rights plaintiffs challenging an unconstitutional voting system have established an injury-in-fact if they can plausibly allege that they face a substantial risk that their votes will not be accurately counted.
2. Whether, at the motion-to-dismiss stage, voting rights plaintiffs challenging an unconstitutional voting system have established that their injuries are fairly traceable to Defendants' conduct when they plausibly allege that Defendants utilize a system that they have failed to properly fortify against risks that the system is vulnerable to attack or failure.

STATEMENT OF CASE

I. Plaintiffs are South Carolina voters whose ability to cast an effective ballot is burdened by Defendants' maintenance of an insecure and outdated voting system.

Plaintiffs Frank Heindel and Phil Leventis are registered South Carolina voters. JA18 ¶¶ 12–13. Each votes regularly in South Carolina elections, and chooses to do so in-person on Election Day at their local precincts in Charleston and Sumter counties, respectively. *Id.* When it is their turn to vote, they are shown to an electronic touchscreen voting machine called an iVotronic. JA20 ¶ 21. After a pollworker loads the appropriate ballot, Mr. Heindel and Mr. Leventis each use the machines' touchscreens to make their selections. JA22 ¶ 27,

JA25 ¶ 36. The voting process is completed with another push of a button, without producing a paper record or other physical evidence that their vote was cast. JA22 ¶ 27. Once they leave the voting booth, their ballots exist only in the memory cards of the voting machines, where they are retrieved by pollworkers at the end of Election Day. JA25 ¶ 37.

This system, certified and maintained by Defendants, places those votes at grave risk. As executive director and commissioners of the South Carolina Election Commission ("SEC"), Defendants have sole responsibility for selecting, purchasing, and certifying the voting machines used across the state. JA20–23 ¶¶ 21–23. Since 2004, they have chosen the iVotronic, a type of paperless electronic voting system known as a Direct Recording Electronic (DRE) machine. JA51 ¶ 109. It is a system that is vulnerable to hacking and prone to mechanical failures, and cannot be meaningfully audited for accuracy. These system failures pose a particularly acute risk at a time when national security officials warn that state election infrastructure continues to be in the cross-hairs of sophisticated adversaries. *See infra* Section V. **Defendants maintain a voting system that is highly vulnerable to hacking.**

As Defendants have been aware for more than a decade, the iVotronic system is exceptionally vulnerable to hacking attacks—and indeed, security researchers long ago hacked it. More than a decade ago, the Ohio Secretary of State commissioned leading computer scientists and academics to analyze the

security of the iVotronic machines, the same machines used in South Carolina. JA26 ¶ 39. Their final report revealed multiple and often easy points of access to install malware into the iVotronic machines and alter the machines' calibration, tabulation, and, ultimately, the election results. *See, e.g.*, JA26 ¶¶ 39–40. In the words of the researchers, the iVotronic could not "guarantee a trustworthy election." JA26 ¶ 40. *See also* JA26 ¶¶ 41-42, JA26 ¶ 44, JA29–32 ¶¶ 50–56.

The many vulnerabilities pervading the iVotronic system provide attackers with opportunities to interfere with election results at a large scale, potentially changing the election results of an entire precinct or county through an attack targeting a single voting machine. Researchers demonstrated these threats in simulated attacks performed directly on the iVotronic equipment, including one they described as "Compromising Entire Election Process with a Virus." JA30 ¶ 52. The iVotronic system relies on hardware components called "Personalized Electronic Ballots," or PEBs, to transfer ballot information and votes between voting machines and the central system. In the simulated attack, researchers used commercially-available personal handheld devices, hacked to function like PEBs, to change data stored on a voting machine. JA26 ¶ 42, JA29 ¶ 51. Due to a software bug, they could introduce software into a single voting machine that could "propagate 'virally'" to other voting machines and back to the central election server via the PEBs—without the system ever connecting to the Internet. JA15

¶¶ 2–3, JA27 ¶ 44, JA29 ¶ 49, JA29 ¶ 50, JA30 ¶ 52, JA31–32 ¶¶ 55–56. In other words, by interacting with a single voting machine, the attacker could launch an attack that would affect all of the votes in a precinct or county. These remarkable findings have been echoed by subsequent studies of the iVotronic system, all of which made it clear—to Defendants and the public—that use of the iVotronic put voters' ballots at risk. JA30–32 ¶¶ 54–56, JA34–35 ¶¶ 63–66.

The inherent unreliability of the iVotronic system is made worse by pervasive flaws in the network security related to South Carolina's election system. JA38–41 ¶¶ 75–82. In 2008, the SEC conducted a security audit that revealed numerous security risks across the state. JA38 ¶ 75. Yet, eight years later, on the eve of the 2016 presidential election, various state and federal agencies engaged by the SEC to test its systems found numerous security issues, some of which were declared "critical." JA39 ¶ 76. Though heavily redacted, the reports of those security tests suggest network security failures that could directly enable the kinds of attacks security researchers have said the iVotronic machine is susceptible to. These failures included problems with the physical security of voting system equipment, as well as vulnerabilities in the software that is used to create ballot definition files and program the voting system. JA23 ¶ 31, JA39 ¶ 77. Although some of these vulnerabilities have been remediated, the pervasiveness of the

deficiencies suggests a more systematic failure to ensure the security of the state's election infrastructure. JA40–41 ¶¶ 79–82.

III. Defendants maintain a voting system that has suffered numerous mechanical failures that cause votes not to be accurately counted.

Separate and apart from its numerous points of vulnerability to attack, the iVotronic machines suffer regular, major mechanical failures that are only getting worse as they age. For more than a decade, the iVotronic system has suffered from mechanical failures that, even in the absence of a malicious cyber-attack, cause votes to go uncounted. Most dramatically, the iVotronic system was used in a 2006 congressional race in Florida in which *18,000 votes cast on iVotronic machines were permanently lost*. JA30 ¶ 54. The fact that the loss of 18,000 votes occurred in a Florida election does not diminish its significance here, because the votes disappeared on the *same system* that Defendants maintain for all South Carolina voters.

Significant mechanical failures—including those resulting in lost votes—have also occurred in South Carolina. Five years ago, a report by South Carolina's Legislative Audit Council identified numerous problems with the state's aging machines. The report summarizes "just a few of the repeated errors in South Carolina," which include, *inter alia*, a 2005 city council primary race in Columbia which initially showed 3,208 total votes, but in which a recount revealed only 768 actual votes. JA35 ¶ 68. An independent study of the reliability of the state's

elections in 2010 "found . . . that Colleton County tallied 13,045 votes when there were only 11,658 ballots cast; Richland County failed to count 1,127 votes; and Charleston, Lancaster, and Orangeburg Counties failed to properly maintain their data, making it impossible to determine whether votes in those counties were correctly counted." JA69 ex. 2, ¶ 10.[1] In the 2018 primary elections, voting machine malfunctions were widespread, causing lines at polls and delaying election results. JA37–38 ¶ 74. For example, in Greenville County, thirty-three machines in four precincts stopped working entirely, and machines broke in at least three other counties. *Id.*

The advanced age of the system used throughout South Carolina makes the risk of future breakdowns more acute. The SEC has conceded that their machines have reached the end of their expected lifespan. JA33 ¶ 61, JA36–37 ¶ 71. In a 2015-16 fiscal year report, the SEC admitted that "[e]quipment issues and breakdowns are becoming more frequent" and as a result "carrying out our mission and reflect[ing] the will of the electorate has become complicated and challenging." JA36 ¶ 70. One local election official described the iVotronic machine as a "dinosaur" that forced county officials to "maintain[] and wring[] out whatever life remains." JA37 ¶ 72.

[1] As noted in the Complaint and its exhibits, Plaintiff Heindel is one of the co-authors of that study.

IV. Defendants maintain a voting system that cannot be meaningfully audited, making it impossible to detect or remediate attacks or lost votes.

If a hacking attack or major system failure occurred, the system offers no manual recount or audit procedure that could detect interference with the software-generated vote count and provide a subsequent remedy. JA41–44 ¶¶ 83–93. The reason for this is simple: Defendants maintain a system that cannot be meaningfully audited, because the iVotronic produces no paper vote record that can be checked against the result stored in the voting machine's memory. JA42 ¶¶ 85–86. Even Defendant Andino has publicly recognized the need for a paper audit trail for any new election machines that the state may purchase in the future. JA42–43 ¶ 88. In its absence, Plaintiffs face the real prospect of casting a ballot that will not ultimately be counted accurately.

V. South Carolina's voting system faces an imminent threat.

The nation's leading intelligence officials, from across the political spectrum, unanimously agree that foreign adversaries are actively and persistently targeting U.S. election infrastructure, including state election systems and the voting-machine manufacturers. JA45–54 ¶¶ 95–114. South Carolina's voting system faces an especially acute and immediate threat. According to a 2018 report by the Senate Select Committee on Intelligence, paperless DRE machines, like those used by Mr. Heindel and Mr. Leventis each Election Day, "are at the highest

risk for security flaws." JA51 ¶ 109. As former CIA director James Woolsey put it, "If I were a bad guy from another country who wanted to disrupt the American system . . . I think I'd concentrate on messing with the touch screen voting systems." JA54 ¶ 114.

Recent history shows that election systems can be vulnerable to hacking attacks by sophisticated foreign actors. In 2016, the Department of Homeland Security documented efforts to attack voter registration records maintained in state election databases. JA46 ¶ 99, JA47 ¶ 102. As many as 21 states may have been targeted, and at least in Illinois, those attacks were successful and the database was breached. JA48 ¶ 103, JA49–50 ¶¶ 105–06. Russian intelligence actors have also targeted voting machine vendors, seeking information about election software and hardware. JA47–48 ¶ 102. Nor is that the sum total of recent attacks on our election infrastructure: as the Senate report explained, states may not have reported all attacks on their equipment, and additional attacks may have gone undetected. JA50–51 ¶¶ 107-08. As the South Carolina State Election Commission itself acknowledged, these events have "created an election-security environment that was very different" than it has been in the past. JA45 ¶ 94. And the intelligence community is clear that the threats have not abated. JA51–54 ¶¶ 111–14. But to date, Defendants have not followed the intelligence community's exhortation to "rapidly replace outdated and vulnerable voting systems." JA51 ¶ 110.

VI. Proceedings in the District Court.

On July 10, 2018, Plaintiffs filed this action in federal district court in South Carolina, seeking declaratory relief and injunctive relief barring the state from continuing to use its aged and faulty iVotronic machines in future elections. On July 30, 2018, Defendants moved to dismiss the complaint. The District Court held argument on that motion on January 15, 2019. On February 8, 2019, the court issued an Order and Opinion granting the motion to dismiss for lack of standing and entered judgment in the case.

In determining whether Plaintiffs had standing, the court found that "Plaintiffs have shown that elections in America have been interfered with, the threat that American elections will be interfered with remains, and that the iVotronic voting machines used in South Carolina are vulnerable to hacking." JA723. Yet the District Court granted the motion to dismiss, finding that "Plaintiffs fail to show that the alleged threatened injury—the possibility that their votes will not be accurately counted due to a hack of South Carolina's voting machines [sic] is *certainly impending*." *Id*. (emphasis in original). Although the District Court acknowledged in a footnote the Supreme Court's holding that standing may be established based on a substantial risk of future harm, *see* JA722–23, it provided no analysis as to whether Plaintiffs' allegations demonstrated a substantial risk that their votes would go uncounted. In ruling against Plaintiffs,

the District Court organized its analysis around the Supreme Court's decision in *Clapper v. Amnesty International*, 568 U.S. 398 (2013). *See* JA722–25, JA728, JA730. It did not explain, however, how the Supreme Court's disposition of the summary-judgment stage showings in *Clapper* should be appropriately applied when deciding a motion to dismiss, where a Plaintiff must plausibly allege an entitlement to relief and well-pled allegations are accepted as true.

SUMMARY OF ARGUMENT

I. Plaintiffs have adequately pled an injury-in-fact. The gravamen of their complaint is that Defendants subject them to a voting system that cannot be relied on to accurately count their vote: it is too vulnerable to hacking—especially in light of the threats targeting U.S. election systems—or mechanical failure. The Supreme Court has made clear that threatened future injury is judicially cognizable when (a) a future harm is "certainly impending" or (b) a plaintiff faces a "substantial risk" that it will materialize. In this case, Plaintiffs have more than plausibly alleged a substantial risk of future injury. Their pleadings detail the profound vulnerabilities of the voting system maintained by Defendants and explain how those vulnerabilities could cause their votes to go uncounted. The District Court, however, failed to apply the proper standard. It explicitly predicated its ruling on the conclusion that Plaintiffs did not establish a "certainly

impending" future harm, but failed to properly consider the substantial risk standard. This was reversible legal error.

II. Plaintiffs' injuries are caused by Defendants and would be redressed by a ruling in their favor. Under South Carolina law, Defendants have sole authority to certify voting systems, and to ensure that any certified voting system complies with all legal requirements. In exercising that authority, they have certified only one voting system, over fifteen years ago, for in-person voters like Plaintiffs, thereby subjecting Plaintiffs to a substantial risk that their votes will not be counted. For the same reason, a favorable ruling would cure those injuries by requiring Defendants to put in place a voting system with reasonable safeguards.

STANDARD OF REVIEW

An appellate court must review *de novo* a district court's granting of a motion to dismiss for failure to establish standing. *Kenny v. Wilson*, 885 F.3d 280, 287 (4th Cir. 2018).

ARGUMENT

For Article III standing, plaintiffs must show—at the pleading stage, through plausible factual allegations—(1) an actual or an imminent injury-in-fact that is concrete and particularized; (2) a causal connection between that injury and the defendant's conduct; and (3) that a favorable judicial decision would likely redress the injury. *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 619

(4th Cir. 2018) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)). Although the injury cannot be "'conjectural' or 'hypothetical,'" "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 414 n.5).

The required showing for standing varies depending on the stage of litigation at which the issue is presented. *See Wikimedia*, 857 F.3d at 208 ("[E]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at successive stages of litigation.") (alterations in original) (citing *Lujan*, 504 U.S. at 561). It is least demanding at the pleading stage, where a litigant must only present well-pleaded allegations that plausibly support his claims. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The district court must accept those allegations as true, and must also assume that a plaintiff will be able to adduce evidence to prove them. For these reasons, it is improper for courts to "inject[] an evidentiary issue into a plausibility determination," *Wikimedia*, 857 F.3d at 212, or "recast[] 'plausibility' into 'probability,'" *id.* at 208.

I. Plaintiffs have pled an injury-in-fact.

A. Defendants' voting system creates a substantial risk that Plaintiffs' votes will not be counted, in violation of their constitutional rights.

1. The failure to have one's vote counted is a cognizable constitutional injury.

Plaintiffs are South Carolina voters facing the imminent risk that their votes will not be counted—that the machines will fail, or be hacked, and when they are, that Plaintiffs' votes will be lost. Depriving Plaintiffs of an effective means to cast a ballot injures them by burdening a core constitutional right.

The U.S. Constitution guarantees each voter's right to an equal and effective vote.[2] A long line of cases emphasizes that states are required to provide an effective right to vote, not merely the formal promise of such a right. *See United States v. Classic*, 313 U.S. 299, 315 (1941) (the right to vote encompasses "the right [of voters] . . . to cast their ballots and have them counted"); *Gray v. Sanders*, 372 U.S. 368, 380 (1963) ("'[T]he right to have one's vote counted' has the same dignity as 'the right to put a ballot in a box.'") (quoting *United States v. Mosley*,

[2] This right emerges from several constitutional provisions, including the Equal Protection Clause, *see, e.g.*, *Reynolds v. Sims*, 377 U.S. 533, 555 (1964); *Gray v. Sanders*, 372 U.S. 368, 379 (1963); *Bush v. Gore*, 531 U.S. 98, 104 (2000); the Due Process Clause, *see, e.g.*, *Anderson v. Celebrezze*, 460 U.S. 780, 787 (1983); the First Amendment, *see, e.g.*, *id.* at 789; *Tashjian v. Republican Party of Connecticut*, 479 U.S. 208, 214 (1986); and Article I, Section II, *see United States v. Classic*, 313 U.S. 299, 315 (1941).

238 U.S. 383, 386 (1915)); *United States v. Weston*, 417 F.2d 181, 183 (4th Cir. 1969) ("The right to vote necessarily includes the right to have one's vote counted and counted at its full worth."); *United States v. Saylor*, 322 U.S. 385, 387–88 (1944) ("[T]he elector's right intended to be protected is not only that to cast his ballot but that to have it honestly counted.") (citing *Mosley*, 238 U.S. at 386). The right to vote is burdened where a state policy creates the risk that some voters will face an arbitrary risk of disenfranchisement, even in the absence of any categorical distinction between voters or any express policy impeding voting. *See Bush*, 531 U.S. at 104–05 ("Having once granted the right to vote on equal terms, the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another."); *Black v. McGuffage*, 209 F. Supp. 2d 889, 899 (N.D. Ill. 2002) (holding that plaintiffs alleged a constitutional violation where some voters would encounter "a system with less accuracy than others"). Thus, when election officials choose a voting system that fails to reliably and accurately count every vote, they put an unconstitutional burden on the right to vote. *See, e.g.*, *Stewart v. Blackwell*, 444 F.3d 843, 868 (6th Cir. 2006), *vac'd as moot following vote for en banc review by* 473 F.3d 692 (6th Cir. 2007); *League of Women Voters of Ohio v. Brunner*, 548 F.3d 463, 468 (6th Cir. 2008); *Common Cause S. Christian Leadership Conference of Greater L.A. v. Jones*, 213 F. Supp. 2d 1106, 1108–09

(C.D. Cal. 2001). Such a burden is unquestionably an injury-in-fact for purposes of standing.

2. Plaintiffs have plausibly alleged that they face a substantial risk that their votes will not be counted.

Plaintiffs need not wait until their votes have been actually discarded to come to court for relief. As noted above, a future injury can establish a plaintiff's Article III standing in one of two ways: "if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Driehaus*, 573 U.S. at 158 (citing *Clapper*, 568 U.S. at 414 n.5). Significantly, standing does not require—as the District Court seemed to assume, *see* JA718—that the future injury be certain. To the contrary, the Supreme Court and lower courts, particularly in the voting-rights context, have applied the "substantial risk" standard to ensure that the threat of future harm can be remedied. For the reasons set out below, Plaintiffs have alleged sufficient facts—which at this stage are uncontested—to plausibly support their claim that they face a substantial risk that their votes will go uncounted because of Defendants' failure to provide a sufficiently reliable voting system.

a) Plaintiffs can plead standing by alleging a substantial risk of injury.

The Supreme Court has made clear that a future injury may be cognizable for Article III purposes when there is a substantial risk that it will materialize. In

Driehaus, for instance, the Supreme Court found that the plaintiffs had standing to challenge future enforcement of a statute criminalizing false statements during a campaign. 573 U.S. at 152–53. The court found there was a substantial risk of enforcement because the statute authorized "'any person' with knowledge of the purported [false statement] to file a complaint," which could harm plaintiffs even if it was ultimately dismissed, and there was "a *real risk* of complaints from, for example, political opponents." *Id.* at 164 (emphasis added). The Court did not demand, and plaintiffs could not show, that their prosecution under the prohibition was "certainly impending." *Id*. at 153–56. While the administrative body charged with enforcing the law had *previously* found probable cause that certain of plaintiffs' statements had violated the law, the political campaigns in which those statements had been made were over. *Id.* And while the plaintiffs alleged that they intended to make similar statements in the future, they also insisted that those statements were true—making it unlikely that they could be convicted of a crime requiring "knowing" falsehoods. *Id*. at 163. Nonetheless, the Court permitted the plaintiffs to pursue their legal challenge because "the threat of future enforcement . . . is substantial." *Id.* at 164.

Similarly, in *Monsanto Co. v. Geertson Seed Farms*, the Court ruled that plaintiffs had standing to challenge a Department of Agriculture regulation based on a substantial risk of harm. The plaintiffs were conventional alfalfa farmers who

sought to stop others from planting genetically modified alfalfa plants. 561 U.S. 139, 153–56 (2010). They asserted that the risk of "gene flow" from the genetically modified alfalfa plants threatened their ability to market their conventional alfalfa crops. *Id.* at 153–54. The district court found that the farmers had "established a 'reasonable probability' that their organic and conventional alfalfa crops will be infected with the engineered gene," which the Supreme Court held to be a sufficiently high risk of injury that the farmers had standing to pursue their challenge. *Id.* at 153–55. *See also State of N.Y. v. U.S. Dep't of Commerce*, 315 F. Supp. 3d 766, 781–85 (S.D.N.Y. 2018) (holding plaintiffs had standing at motion-to-dismiss stage when they could plausibly allege concrete facts to support their assertion of a substantial risk of injury); *State of N.Y. v. U.S. Dep't of Commerce*, 351 F. Supp. 3d 502, 575 (S.D.N.Y. 2019) ("[I]n regulating the federal courts' power to dispense prospective relief, Article III is concerned with the *risk* of future injury, rather than its ultimate realization.") (emphasis in original).

It is especially clear that voters have standing when they face a substantial risk of losing their voting rights. Courts routinely assess voters' challenges to election procedures without waiting to see which specific votes will be impeded by a challenged policy. *See, e.g.*, *League of Women Voters of N.C. v. North Carolina*, 769 F.3d 224, 230 (4th Cir. 2014) (enjoining enforcement of new election procedures in North Carolina based on risk that some voters would be injured). If

courts did not do so, they would risk leaving voters with no remedy at all, as the Supreme Court has explained: "Challengers to election procedures often have been left without a remedy in regard to the most immediate election because the election is too far underway or actually consummated prior to judgment." *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 300 n.12 (1979).

Courts considering claims by voters asserting a threat of disenfranchisement have generally found an injury-in-fact when voter-plaintiffs (1) identify a policy that will operate in elections in which they will participate, (2) plausibly allege a risk that the challenged policy will deprive them of their right to vote, and (3) assert claims in a context where there is no realistic way to predict with certainty whether their specific votes will be affected. This approach can be seen in numerous cases holding that voters have standing to challenge practices whose impact on their specific ability to vote is uncertain. For example, in *Arcia v. Fla. Sec'y of State*, 772 F.3d 1335, 1341 (11th Cir. 2014), the Eleventh Circuit held that voters could seek an injunction stopping Florida's voter-purge practices without waiting until they were actually purged from the rolls. Though voters had been mistakenly identified as non-citizens by a prior iteration of the voter purge program, they were ultimately able to vote in the previous election. *Id.* While they were not certain they would be purged again, the court held that there was a "realistic probability" that they would be. *Id.* Ruling in plaintiffs' favor, the court

explained that, "[w]hile the threatened future injury cannot be merely hypothetical or conjectural, probabilistic harm is enough." *Id.* That is, they did not have to show that they were actually deprived of their right to vote in past elections, or that they were certain to be deprived of the right in future elections, to have standing to pursue their claims.

A recent ruling from the Northern District of Georgia—in a case raising claims that closely mirror this case—illustrates the proper application of standing principles in a case involving substantial risk to the effectiveness of a plaintiff's vote posed by an insecure voting system. In *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1316 (N.D. Ga. 2018), the plaintiffs were voters challenging the constitutional adequacy of Georgia's election system. As in South Carolina, all polling places in Georgia use paperless DRE machines that produce no paper record. *Id*. at 1307. That system also suffers from significant security flaws resulting from vulnerabilities in its architecture and software. *Id.* at 1308. Additionally, election officials responsible for maintaining the system had failed to observe basic norms of cybersecurity. *Id.* at 1324. Plaintiffs in *Curling* claim that the continued use of Georgia's DRE-based system violates their right to vote under the Due Process Clause and Equal Protection Clause of the Fourteenth Amendment. *Id.* at 1312. In denying the motion to dismiss, the court found standing based on "the threat of future harm," because "[p]laintiffs plausibly allege

a threat of a future hacking event that would jeopardize their votes and the voting system at large." *Id*. at 1316. It emphasized in particular that "courts have found that plaintiffs have standing to bring Due Process and Equal Protection claims where they alleged that their votes would likely be improperly counted based on the use of certain voting technology." *Id*.

Similarly, a district court in this circuit recently recognized, applying *Clapper*, that a voter has standing to challenge election policies based on a showing of substantial risk of harm, even if she cannot show that the harm was certain to occur. *See N.C. State Conference of NAACP v. N.C. State Bd. of Elections*, 283 F. Supp. 3d 393, 403–04 (M.D.N.C. 2017). In that case, plaintiffs challenged a state law allowing third parties to challenge a voter's registration based solely on a single undelivered piece of mail addressed to the voter's home address. *See N.C. State Conference of NAACP v. N.C. State Bd. of Elections*, 2016 WL 6581284, at *5–7, *10 (M.D.N.C. Nov. 4, 2016) (describing allegations in complaint). Denying a motion to dismiss, the court held that a voter had standing to challenge this practice in his county even though he had not been "purged from the rolls or prevented from voting." 283 F. Supp. 3d at 403. The court recognized that the existence of the policy, coupled with factual allegations explaining why the policy was likely to be used in future election, gave rise to a "substantial risk of future harm" supporting the voter's standing. *Id*. at 404.

The application of the substantial risk standard in recent cases reflects the longstanding approach to voting rights cases premised on a substantial risk of future injury. For example, in *ACLU of N.M. v. Santillanes*, 546 F.3d 1313, 1319 (10th Cir. 2008), the Tenth Circuit allowed a challenge to a voter ID policy to proceed before any voter had been directly affected by the policy. The plaintiffs were New Mexico voters who were uncertain whether their photo identification would pass muster under the new voter ID law. *Id.* at 1318. The court acknowledged that, "[a]s in many cases challenging aspects of voting, Plaintiffs cannot identify a single individual who would not vote, let alone not vote in-person because of the measure." *Id.* at 1319. Nonetheless, the court determined that the plaintiffs' photo identification could "confound election judges, *potentially* result in arbitrary enforcement of the requirement, and result in unequal treatment as compared to those who vote absentee." *Id.* (emphasis added). That potential for arbitrary treatment was enough, the court held, for the voters to have standing to bring their constitutional challenge. *Id.* The same foundational principles have led courts to allow plaintiffs to challenge the use of allegedly unreliable voting machines,[3] provisional ballot procedures,[4] and changes to straight-ticket voting

[3] *See Stewart*, 444 F.3d at 854 (finding voters have standing to challenge voting systems based on "an increased risk that their votes will be improperly discounted"); *Black*, 209 F. Supp. 2d at 894 (allowing plaintiffs to challenge punch card-based voting system based on "disproportionate risk of having their votes not counted").

rules[5] without requiring that the plaintiffs demonstrate that any particular voter will certainly be injured by the election policies.

b) Plaintiffs have alleged a substantial risk of injury.

Plaintiffs have clearly shown that they have standing to challenge South Carolina's outdated and insecure voting system. Consistent with the cases described above, Plaintiffs have alleged that (1) they are subject to the challenged system (the only one approved by Defendants for in-person voters in South Carolina); (2) the defects in that system place their votes at substantial risk of going uncounted; and (3) it is impossible to know with certainty which votes will be affected in future elections, or (because of the lack of audits) to confirm whether votes have been accurately counted.

First, there is no question that Plaintiffs are subject to the voting system at issue here. Under current South Carolina law, the iVotronic system is the only voting system certified by the SEC for use in South Carolina for in-person voting. JA20–23 ¶¶ 21–31. Plaintiffs are South Carolina voters who are regular Election

---

[4] *See Sandusky Cty. Democratic Party v. Blackwell*, 387 F.3d 565, 574 (6th Cir. 2004) (per curiam) (finding that voters had standing to challenge Ohio's provisional ballot procedures before the election took place, even though plaintiffs had not "identified specific voters who will seek to vote at a polling place that will be deemed wrong by election workers").

[5] *Mich. State A. Philip Randolph Inst. v. Johnson*, 209 F. Supp. 3d 935, 940 (E.D. Mich. 2016), *stay pending appeal denied*, 833 F.3d 656 (6th Cir. 2016) (allowing plaintiffs to challenge Michigan law abolishing straight-ticket voting based on risk of increased wait times).

Day in-person voters, and therefore can expect to use iVotronic machines in upcoming elections, including the 2020 presidential primaries and general elections. JA18–19 ¶¶ 12–13.

Second, as the complaint alleges in detail, there is a substantial risk that the iVotronic system will fail to accurately count Plaintiffs' votes, due to either hacking or mechanical failure. Since 2016, national security and intelligence leaders have repeatedly made clear that foreign actors intend to interfere with U.S. election systems in upcoming elections. JA45–54 ¶¶ 95–114. Contrary to the District Court's assertion, *see* JA728, Plaintiffs have alleged facts to show that the risk continued, rather than diminished, after 2016. Both then-CIA Director Mike Pompeo and then-Secretary of State Rex Tillerson reported that Russian efforts were highly likely to continue in 2018. JA51–52 ¶ 111. Intelligence chiefs later confirmed that this meddling did actually occur. JA52–53 ¶ 112. And paperless electronic voting machines like the iVotronic are the principal target of that threat. JA51 ¶ 109. As Ambassador James Woolsey, former director of the CIA, put it in a 2016 interview: "If I were a bad guy from another country who wanted to disrupt the American system . . . I think I'd concentrate on messing up the touch screen voting systems." JA54 ¶ 114. South Carolina is one of five remaining states that uses such systems for all in person voting. JA51 ¶ 109.

If hackers do try to breach the iVotronic system, they are likely to succeed, as a direct result of Defendants' choice of system and security measures. Defendants have known since at least 2007 that the iVotronic system is highly vulnerable to hacking attacks. JA26–30 ¶¶ 39–52. As described in detail in the Complaint, leading security researchers have successfully hacked the iVotronic system and exploited vulnerabilities that, in a real election, would allow them to change votes on a large scale. JA23 ¶ 29. Critically, the networked structure of the iVotronic means that a single attack can affect voters at a large scale by "propagat[ing] 'virally' from the field back to the county election management system." JA29–30 ¶¶ 49, 52. The history of the iVotronic system's exposure to potentially devastating attacks strongly supports the plausibility of Plaintiffs' allegations that they face a substantial risk of future attacks that impedes their right to vote. *See Curling*, 334 F. Supp. 3d at 1314 (finding non-speculative injury where voters challenged Georgia's paperless DRE system and "the DRE voting system was *actually* accessed or hacked multiple times already—albeit by cybersecurity experts who reported the system's vulnerabilities to state authorities, as opposed to someone with nefarious purposes").[6]

[6] The District Court's analysis suggests that the previous hacking of Georgia's machines distinguishes *Curling* from this case, *see* JA737–38 n.24, but that distinction is untenable. In both cases, security researchers detected serious vulnerabilities with the relevant DRE voting system and reported those vulnerabilities to election officials and eventually the public, without actually

All of these vulnerabilities are compounded by network security failures that directly increase the risk of the iVotronic system being hacked. JA38–44 ¶¶ 75–93. The South Carolina National Guard Defensive Cyber Operations Element found that, in the lead up to the 2016 elections, 20 of 46 counties had "critical" vulnerabilities related to the Unity software, which works in conjunction with the iVotronic firmware to tally election results, and that 21 counties had physical security vulnerabilities. JA22 ¶ 26, JA39 ¶ 77. A Department of Homeland Security review of the SEC's system found numerous "critical" and "high" level vulnerabilities. JA40 ¶ 79. These kinds of vulnerabilities exacerbate the inherent security flaws in the iVotronic system. Failures in physical security could enable an attack on a voting machine or another component of the system, with the prospect of such an attack "propagating virally" throughout a precinct or county. JA29 ¶¶ 49–50. Critical vulnerabilities in the county-based Unity software system similarly increase the risk of a large scale attack, since the Unity system is used at county election headquarters to, among other things, design ballots, program components of the system, and tabulate election results. JA23 ¶ 31. Because files are transferred from the Unity system to the voting machines and other

---

interfering with any votes. *Compare* JA25–32 ¶¶ 38–56 *with Curling*, 334 F. Supp. 3d at 1310. From the perspective of the risk of future injury, the prior breaches of each state's election system have the same significance. In both cases, they presage future attacks that have the potential to prevent accurate vote counting.

components of the iVotronic system, an attacker could use malware introduced through Unity to infect the entire system. These additional layers of insecurity reinforce the plausibility of Plaintiffs' allegations that they face a substantial risk that their votes will be rendered ineffective.

Moreover, the system has a significant history of repeatedly failing to count all votes in live elections. The most glaring example is the loss of 18,000 votes in a Florida congressional race using the iVotronic system. Though that election took place in a different jurisdiction, it used the same iVotronic system at issue here. JA30–31 ¶ 54. South Carolina's iVotronic machines have also failed repeatedly over the years. JA35–36, 37–38 ¶¶ 68, 74. In 2010, for instance, Colleton County tallied approximately 1,500 more votes than there were voters who cast ballots, and Richland County failed to count 1,127 votes. JA68. Three other counties failed to properly maintain their data, making it "impossible to determine" whether the vote count within the system was internally consistent. *Id.* Those failures will only become more frequent as the system ages, leaving voters with a system that (as Defendants admit) has passed its expiration date, and cannot be readily repaired. JA33 ¶ 61, JA36–38 ¶¶ 69–74.

Third, the nature of the risks involved makes it impossible to know with certainty which voters will be disenfranchised by a hack or mechanical failure, and Defendants' failure to provide for meaningful audits makes it impossible to

reliably detect hacking or mechanical failure. It is of course true that predicting when a machine will erase votes, or when and how a foreign adversary will attack, is impossible—and for that reason, Plaintiffs cannot allege that an attack that impacts their specific votes is literally certain to occur. Similarly, Defendants' failure to provide for meaningful audit systems that would detect cyber-attacks or errors may make it impossible to know with certainty *even in retrospect* whether a hack or mechanical failure has occurred. JA41–44 ¶¶ 83–93. But this does not place Plaintiffs' allegations beyond the ambit of Article III; to the contrary, it places them squarely in line with cases in which courts have acknowledged that, in the voting context, a substantial risk of harm supports standing precisely because it is impossible to predict in advance which voters will wrongfully lose their right to vote. *See Arcia*, 772 F.3d at 1341; *Santillanes* 546 F.3d at 1319.

***

Under these circumstances, Plaintiffs face a substantial risk that their votes will not be counted. *See, e.g.*, *Curling*, 334 F. Supp. 3d at 1316 ("Plaintiffs plausibly allege a threat of a future hacking event that would jeopardize their votes and the voting system at large."). That is a profound injury, and under governing doctrine it suffices to establish standing at this stage of the case.

c) The District Court applied an incorrect legal standard to Plaintiffs' claims and relied on inapt precedents.

The District Court, in reaching a contrary conclusion, applied the wrong standard. Specifically, the District Court examined the issues in this case almost entirely through the lens of the "certainly impending" prong of the standard identified in *Clapper* and *Driehaus*, without giving meaningful attention to the line of cases—including *Clapper* itself—permitting plaintiffs to establish standing on the basis of a "substantial risk" of future injury. The District Court acknowledged the substantial risk standard primarily in a footnote, but failed to explain in that footnote or elsewhere how it applied the substantial risk standard to the allegations advanced by Plaintiffs. *See* JA722–23 n.14.[7] Rather than even purport to apply that standard to Plaintiffs' allegations, the District Court stated that it was ruling against Plaintiffs based on the conclusion that they failed to allege a *certainly impending* future injury. *See* JA724 at 16 ("However, Plaintiffs fail to show that

[7] The District Court's footnote discussion concludes by suggesting that a substantial risk may only be considered when it "'prompts plaintiffs to reasonably incur costs to mitigate or avoid that harm.'" JA723 n.14 (quoting *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017)). That view is not supported by the case law. But in any event, Plaintiffs *have* alleged that one of them, Frank Heindel, has in fact undertaken reasonable costs to avoid the risks of voting on the insecure system maintained by the Defendants. *See* JA18–19 ¶ 12 & JA66–73 ¶¶ 4–22. In addition to this footnote discussion, the District Court summarily stated that Plaintiffs' hacking theory "is also too attenuated to satisfy the substantial risk of harm standard," but did not explain why, or examine Plaintiffs' allegations in light of that standard. JA732.

the alleged threatened injury—the possibility that their vote will not be accurately counted due to a hack of South Carolina's voting machines is *certainly impending*.") (emphasis in original).

The District Court's erroneous application of the certainly impending standard is highlighted by its extensive reliance on the Supreme Court's decision in *Clapper*, despite dipositive differences between the two cases. Indeed, the District Court effectively enlisted *Clapper* as the organizing framework for its analysis. *See* JA722–25, 728, 730–32. But comparing this case to *Clapper* reveals just how inapt the District Court's framework is in this case. *Clapper* involved a challenge to a specific surveillance statute, 50 U.S.C. § 1881a, by U.S. persons and organizations who feared that their international correspondence with likely targets of U.S. surveillance would be intercepted. 568 U.S. 406–07. In ruling that those plaintiffs had failed to establish standing at the summary-judgment stage, the Court identified several ways in which the plaintiffs had failed to adduce specific facts to support the inferences required to find that the risk of harm was substantial—in stark contrast to the allegations at issue here. For example:

- The Court ruled that it was speculative whether the plaintiffs' international correspondence would be subject to the surveillance statute at issue. *Id*. at 411. Here, Plaintiffs have alleged that (1) U.S. election systems in general, and South Carolina's paperless DRE systems in particular, have been

deemed by the country's intelligence and national-security officials to be active targets of hacking; (2) that the iVotronic system has in fact been hacked (by security researchers); and (3) that the iVotronic system has in fact failed to count votes in live elections.

- In *Clapper*, the plaintiffs were forced to speculate as to whether § 1881a—the statute they sought to challenge—would be the particular legal authority used for any surveillance affecting them, since the government had an array of other surveillance authorities capable of similar uses but beyond the scope of the lawsuit, *id.* at 412–13; in this case, Plaintiffs have alleged that the challenged voting system is currently the only one authorized for in-person South Carolina voters like them.
- The *Clapper* plaintiffs' injuries would materialize only if the FISA court's Article III judges failed to act as a safeguard and authorized an unconstitutional surveillance application, *id.* at 410; in this case, there is no comparable intervening safeguard, and indeed, plaintiffs have alleged that safeguards that should exist have faltered (network security) or simply do not exist (meaningful audits).
- Finally, the Court reasoned that the *Clapper* plaintiffs could only speculate as to whether the government would succeed in obtaining any targeted communications and whether, even if it did, it would sweep up plaintiffs'

own correspondence in that surveillance (since they alleged that it was their foreign contacts, not them, who would be the direct targets of §1881a surveillance). Though it is true in this case that Plaintiffs cannot allege that their specific votes will certainly be implicated in a future hacking or mechanical failure, the different context of the two cases is significant. In *Clapper*, the Supreme Court was understandably reluctant to speculate as to how "the Attorney General and the Director of National Intelligence will exercise their discretion." *Id*. at 412. In contrast, Plaintiffs here allege an assessment of risk that does not require speculation or second-guessing of national-security officials, but instead is premised on the public assessments of the country's top intelligence and national-security officials. Further, this case alleges an injury to voting rights, which courts have repeatedly held to be cognizable even when a plaintiff does not know with certainty whether his vote will be affected by a challenged policy. *See Curling*, 354 F. Supp. 3d at 1319 (distinguishing *Clapper* where "fundamental rights, such as the right to vote," are threatened).

The District Court's reliance on *Clapper* is particularly inapt because *Clapper* concerned a challenge to standing at the summary-judgment stage, and the Court therefore held the plaintiffs to the more demanding summary-judgment standard. This Court has previously cautioned against using *Clapper*'s summary-

judgment standard in cases at the motion-to-dismiss stage: "[W]hat may perhaps be speculative at summary judgment can be plausible on a motion to dismiss." *Wikimedia*, 857 F.3d at 212. For that reason, this Court has admonished district courts against "blurring the line between the distinct burden for establishing standing at the motion-to-dismiss and summary-judgment stages of litigation." *Id*. When, as here, plaintiffs ground their "detailed" allegations in "publicly disclosed information" that support their claim about the risk of injury, that is not "speculative" at the motion-to-dismiss stage. *Id.*

In concluding that Plaintiffs' alleged injury is too speculative to constitute an injury-in-fact, the District Court also relied heavily on this Court's decision in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017). *See* JA724–28. *Beck* was an appeal in two consolidated cases. In one, a laptop computer containing personal data of approximately 7,400 patients was "likely stolen" from a hospital. 848 F.3d at 267. The second involved the theft of hard copies of approximately 2,000 pathology reports and the personal patient data included in those reports. *Id.* at 268. More than three years after these thefts, there was no indication that any of the data had been misused, or even accessed. *See id*. at 267–68, 274–75. The plaintiffs did not allege that the thief had "intentionally" stolen the laptop or pathology in order to misuse their personal information, nor did they allege any misuse had actually occurred. Nevertheless, plaintiff-patients argued that the hospital's loss of the data

placed them at an increased risk of identity theft. *See id*. at 274–75. The *Beck* panel held that "the mere theft of [the laptop and pathology reports], without more, cannot confer Article III standing." *Id*. at 275.

The District Court's reliance on *Beck* was misplaced for two reasons:[8]

First, *Beck* involved the theft of material that contained potentially sensitive data, without any allegation that the thieves stole those items because they *intended* to exploit the data they happened to capture. In distinguishing earlier cases finding standing in data-breach cases, the court drew a contrast with cases involving allegations of *intent* to misuse data. *Id*. at 274. In *Beck*, such intent was not self-evident—one can certainly imagine a thief who steals a laptop for reasons other than exploiting the personal data it happens to contain. The lack of intent to exploit the data, in the court's view, rendered the risk of injuries flowing from the exploitation of that data overly speculative. *Id*. In contrast, Plaintiffs have alleged concrete facts showing that sophisticated adversaries *specifically intend* to attack and disrupt U.S. elections, JA53–54 ¶¶ 111–14, and that such risks are especially pronounced in states, like South Carolina, that rely on aging, paperless DRE machines, JA53–54 ¶¶ 109, 114. And of course, Plaintiffs here allege that the risk of injury arises not only from the (imminent and acute) risk of malicious hacks, but

[8] Plaintiffs note that *Beck* was not cited in any of the briefing before the District Court, nor was it raised at argument, so Plaintiffs were never presented below with an opportunity to dispute *Beck*'s relevance to this case.

the *combined risk* of hacks and mechanical failure. JA35–37 ¶¶ 67–74, JA68–69 ¶ 10.

Second, in *Beck*, the court drew an inference about the decreased risk of injury based on the time elapsed since the theft of the property containing personal data. No similar inference can be drawn here. The *Beck* Court reasoned that "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275 (citations omitted). The District Court explicitly relied on that proposition here, finding that "as the 'events leading up to the 2016 election,' (ECF No. 14 at 15), 'fade further into the past[,]' . . . Plaintiffs' threatened injuries become more and more speculative." JA726 (quoting *Beck*, 848 F.3d at 275). This misapplies *Beck*. The court in *Beck* proceeded from the assumption that the risk of future harm arising from stolen data becomes steadily more remote with time—where the information apparently obtained by thieves has not been misused after a period of years, that supports an inference that it will not be misused at some indefinite point in the future. That assumption is clearly unwarranted in the context of elections, where the risk tracks the election calendar. It can be plausibly inferred that the actors who targeted American elections in 2016 and 2018, *see* JA44–54 ¶¶ 94–114, will continue to do so in 2020. The first presidential race since the 2016 election is fast approaching; for that reason, it is untenable to assume, as the District Court did, that the risk of

hacking decreases as that new election cycle approaches. Moreover, assuming a steadily decreasing risk makes little sense here, where the risk of voting machine breakdown *increases* with the age of the machines. Because the South Carolina election system, as Defendants agree, "is approaching end of life" and has not been replaced, JA33 ¶ 61, the more time passes, the more antiquated and vulnerable to failure the voting system becomes.

The District Court also identified three district-court cases that it described as "mirror[ing] Plaintiffs' claims" and supporting dismissal. JA739 (citing *Stein v. Cortes*, 223 F. Supp. 3d 423 (E.D. Pa. 2016); *Landes v. Tartaglione*, 2004 WL 2415074 (E.D. Pa. Oct. 28, 2004); *Schulz v. Kellner*, 2011 WL 2669456 (N.D.N.Y. July 7, 2011)). They do not. Instead, these cases stand for the uncontroversial requirement that plaintiffs must allege and show more than a theoretical possibility of harm to a legally protected interest. For example, in *Stein v. Cortes*, the plaintiffs were unsuccessful 2016 presidential candidate Jill Stein and one Pennsylvania voter. 223 F. Supp. 3d at 426. The plaintiffs arrived in federal court after several unsuccessful attempts to convince state courts to require a forensic examination of DRE machines, a remedy neither mandated nor permitted under state law. *Id.* at 426–29. The *Stein* plaintiffs offered only conclusory allegations that Pennsylvania's DRE machines were vulnerable, and sought to undo the results of a completed election without any evidence that those

election results had been compromised. Here, by contrast, Plaintiffs seek only prospective relief, based on detailed, plausible allegations of (1) the vulnerability of South Carolina's voting machines to hacking and malfunction and (2) the high risk that foreign actors will in fact seek to hack an election. In the other two cases, *pro se* plaintiffs alleged—without specific factual support—that voting machines and nontransparent voting procedures were per se unconstitutional. Am. Compl. ¶ 246, *Schulz* (No. 1:07–CV–943) ("Voting procedures that are not open, verifiable, transparent and machine and computer free . . . abridge the right to cast an effective vote."); Compl. ¶ 23, *Landes* (No. 04–CV–3163) (arguing that voting machines violated Constitution because they, rather than voters, "physically mark, cast, and count the ballots"). Dismissal was warranted because the plaintiffs either failed to show a legally cognizable interest, *Schulz*, 2011 WL 2669456, at *5 (concluding plaintiffs lacked a "legally protected interest in having their votes counted manually and in full public viewing"), or to actually allege the injury, *id.* at *7 ("Plaintiffs have not presented any concrete or specific factual allegations from which the Court could infer" the injury has occurred or will occur); *Landes*, 2004 WL 2415074, at *3 (plaintiff failed to show injury in fact where "she d[id] not assert that the voting machines have actually suffered from these issues in the past" or would in future). These cases hardly support dismissal of the detailed and specific allegations presented here.

B. Plaintiffs face a particularized, concrete injury, not a generalized grievance.

Plaintiffs seek relief for a quintessentially personal and concrete injury: a burden on their right to vote. To be particularized, an injury must "affect the plaintiff in a personal and individual way." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1543 (2016) (quoting *Lujan*, 504 U.S. at 560 n.1). That does not mean that a plaintiff's injuries must be unique: "[W]here a harm is concrete, though widely shared, the Court has found 'injury in fact.'" *Fed. Election Comm'n v. Akins*, 524 U.S. 11, 24 (1998). As the Supreme Court explained in *Akins*, a situation "where large numbers of voters suffer interference with voting rights conferred by law" is a paradigmatic example of a widely shared injury that is sufficiently concrete to support standing. *Id*. Consistent with *Akins*, this Court has recognized that a burden on the right to vote is "a concrete harm" to an individual sufficient to support Article III standing, even when other voters are injured in the same or similar ways. *Bishop v. Bartlett*, 575 F.3d 419, 425 (4th Cir. 2009). Plaintiffs here have alleged injuries to the effectiveness of *their own votes*; that is sufficiently particularized to support standing here.

The District Court's contrary conclusion misapprehends what constitutes a generalized grievance. The court concluded that "as Plaintiffs' allegations are not personal to Plaintiffs, and could be advanced by any South Carolina voter, Plaintiffs' 'asserted harm is a "generalized grievance" shared in substantially equal

measure by all or a large class of citizens.'" JA743 (quoting *Warth v. Seldin*, 422 U.S. 490, 499 (1975)). But the fact that this injury is widely shared does not diminish the concreteness of the injury to Plaintiffs—indeed, it is precisely the situation described by the Court in *Akins* as paradigmatically *not* a generalized grievance. It stands in stark contrast to the nonjusticiable generalized grievances that anyone might bring to vindicate abstract injuries, like concern for a municipal treasury's solvency or society's obedience to law. *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 344 (2006). Plaintiffs' injury is neither abstract nor undifferentiated. Rather, they assert "a plain, direct, and adequate interest in maintaining the effectiveness of *their* votes." *See Judge v. Quinn*, 612 F.3d 537, 545 (7th Cir. 2010) (emphasis added) (internal quotation omitted). This Court has already rejected the argument that a deprivation of the right to vote is a generalized grievance. *Bishop*, 575 F.3d at 424–25. Indeed, the consequence of the District Court's logic would be untenable: a state would become free to enact any policy that burdens voting rights so long as it cast a wide enough net in doing so.

II. Plaintiffs satisfy the causality and redressability standards.

A. Plaintiffs plausibly allege that their injuries are fairly traceable to Defendants' conduct.

In addition to establishing a substantial risk of injury, a plaintiff must demonstrate "a causal connection between the injury and the conduct complained of—the injury has to be fairly . . . trace[able] to the challenged action of the

defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (internal quotation omitted). The Supreme Court has held that establishing the "traceability" of a plaintiff's injury to a defendant's conduct does not require that the defendant be the sole or even proximate cause of that injury. To the contrary, the causal connection can be satisfied even if a third party plays a role in causing a plaintiff's injury. *See, e.g.*, *Driehaus*, 573 U.S. at 151–53, 164 (finding standing to challenge restriction on false political statements where private complainants not before the court initiate enforcement proceedings).

In the election-law context, "[i]mposition of the stringent proximate cause standard . . . has been held to 'wrongly equate . . . injury fairly traceable to the defendant with injury as to which the defendant's actions are the very last step in the chain of causation.'" *Libertarian Party of Va. v. Judd*, 718 F.3d 308, 315–16 (4th Cir. 2013) (quoting *Bennett v. Spear*, 520 U.S. 154, 168–69 (1997)). For example, in *N.C. State Conference of NAACP*, the plaintiff would have been injured by the defendant's voter-purge policy only if his voter registration status was actually challenged by a third party. 283 F. Supp. 3d at 404. The risk was nonetheless traceable to defendants' actions because they set the policy that "enabl[ed] challengers to bring systematic, coordinated, *en masse* challenges to large numbers of registered voters." *Id.* (quoting complaint). As a general matter,

as long as the challenged election-related conduct "is at least in part responsible" for the plaintiff's injury, the fairly traceable standard is satisfied, "notwithstanding the presence of another proximate cause." *See Judd*, 718 F.3d at 316. *See also Constitution Party of Pa. v. Aichele*, 757 F.3d 347 (3d Cir. 2014) (minor party had standing to challenge Pennsylvania ballot-access rule even though it could be injured only if a third party challenged signatures on party's petition).

The District Court failed to apply this precedent properly. It noted that, because Plaintiffs "do not allege [Defendants] would be the 'potential' hackers, the potential hackers must be 'some third party not before the court.'" JA733 (quoting *Lujan*, 504 U.S. at 560 (internal quotation omitted)). For this reason, the District Court concluded, the alleged injury was not fairly traceable to Defendants. *Id.* (quoting *Lujan*, 504 U.S. at 560). This was clear legal error. A defendant need only be "at least in part responsible" for the alleged injury. *Judd*, 718 F.3d at 316. Defendants are the officials responsible for maintaining an election system capable of effectively recording and counting votes, and for changing course if the system in place fails to do so. JA55 ¶¶ 118–20. Despite being on notice since at least 2007 that the iVotronic system is severely vulnerable to manipulation—and faced with a unanimous chorus of national-security experts warning of the dangers posed by foreign hackers—Defendants have continually failed to replace the system. JA17–18 ¶ 10, JA33 ¶ 61, JA36–37 ¶ 71, JA56 ¶ 124. Any injury sustained by

Plaintiffs resulting even in part from these deficiencies is thus fairly traceable to Defendants. Moreover, the District Court's traceability discussion addresses only the risk of hacking, and wholly ignores the additional risk of iVotronic machine malfunction. There is no question that this aspect of the risk to Plaintiffs' votes is directly traceable to Defendants' failure to replace the flawed, aging system, despite their acknowledgment that it is well past time to do so.

B. Plaintiffs plausibly allege that their injuries will be redressed by a court order.

Redressability is "a likelihood that the requested relief will redress the alleged injury." *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 103 (1998). As this Court has explained, "[t]he redressability requirement ensures that a plaintiff 'personally would benefit in a tangible way from the court's intervention.' A plaintiff seeking injunctive relief shows redressability by 'alleg[ing] a continuing violation or the imminence of a future violation'. . . ." *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 162 (4th Cir. 2000) (quoting *Warth*, 422 U.S. at 508; *Steel Co.*, 523 U.S. at 108) (internal citation omitted) (alteration in original).

Defendants are the sole officials responsible for selecting and certifying election systems for South Carolina. JA55 ¶¶ 118–20. Plaintiffs seek in this litigation to require them to replace the current system—which burdens their right to vote—and replace it with a sufficiently reliable and accurate system. Obtaining

such relief would ensure that Plaintiffs have access to a voting system that will ensure the effectiveness of their ballots.

CONCLUSION

For the foregoing reasons, the Court should reverse the District Court's ruling and remand the case for further proceedings.

REQUEST FOR ORAL ARGUMENT

Pursuant to Local Rule 34(a), Plaintiffs respectfully request that this Court grant them oral argument due to the important, constitutional issues presented by this appeal.

April 8, 2019

Respectfully submitted,

/s/ Laurence M. Schwartztol

Laurence M. Schwartztol
PROTECT DEMOCRACY PROJECT, INC.
125 Walnut Street, Suite 202
Watertown, Massachusetts 02472
Telephone: 202.945.2092
Facsimile: 929.777.8248
larry.schwarztol@protectdemocracy.org

Jessica Marsden
PROTECT DEMOCRACY PROJECT, INC.
510 Meadowmont Village Circle, No.328
Chapel Hill, North Carolina 27510
Telephone: 202.672.4812
Facsimile: 929.777.8428
jess.marsden@protectdemocracy.org

Jamila Benkato
PROTECT DEMOCRACY PROJECT, INC.
2020 Pennsylvania Avenue, NW, Suite #163
Washington, D.C. 20006
Telephone: 202.856.9191
Facsimile: 929.777.8428
jamila.benkato@protectdemocracy.org

David S. Frankel
Harry P. Morgenthau
KRAMER LEVIN NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
Telephone: 212.715.9100
Facsimile: 212.715.8000
dfrankel@kramerlevin.com
hmorgenthau@kramerlevin.com

Counsel for Plaintiffs-Appellants

CERTIFICATE OF COMPLIANCE

In accordance with Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure, the undersigned counsel for Plaintiffs-Appellants certifies that the accompanying brief is printed in a proportionally spaced Times New Roman typeface, 14-point, and that the text of the brief comprises 10,858 words according to the word count provided by Microsoft Word, excluding the parts of the document excepted by Fed. R. Civ. P. 32(f).

/s/ Laurence M. Schwartztol

Laurence M. Schwartztol
PROTECT DEMOCRACY PROJECT, INC.
125 Walnut Street, Suite 202
Watertown, Massachusetts 02472
Telephone: 202.945.2092
Facsimile: 929.777.8248
larry.schwarztol@protectdemocracy.org

CERTIFICATE OF SERVICE

I certify that on April 8, 2019, the foregoing document was served on all parties or their counsel of record through the CM/ECF system.

/s/ Laurence M. Schwartztol

Laurence M. Schwartztol
PROTECT DEMOCRACY PROJECT, INC.
125 Walnut Street, Suite 202
Watertown, Massachusetts 02472
Telephone: 202.945.2092
Facsimile: 929.777.8248
larry.schwarztol@protectdemocracy.org